(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
6. Februar 2003 (06.02.2003)

PCT

(10) Internationale Veröffentlichungsnummer
WO 03/010919 A1

(51) Internationale Patentklassifikation: H04L 9/06

(21) Internationales Aktenzeichen: PCT/EP02/07296

(22) Internationales Anmeldedatum:
2. Juli 2002 (02.07.2002)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
101 36 303.6 26. Juli 2001 (26.07.2001) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **INFINEON TECHNOLOGIES AG** [DE/DE]; St.-Martin-Str. 53, 81669 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **BIER, Peter** [DE/DE]; Albrechtstr. 2, 85551 Kirchheim (DE). **JANKE, Marcus** [DE/DE]; Spitzingplatz 3, 81539 München (DE).

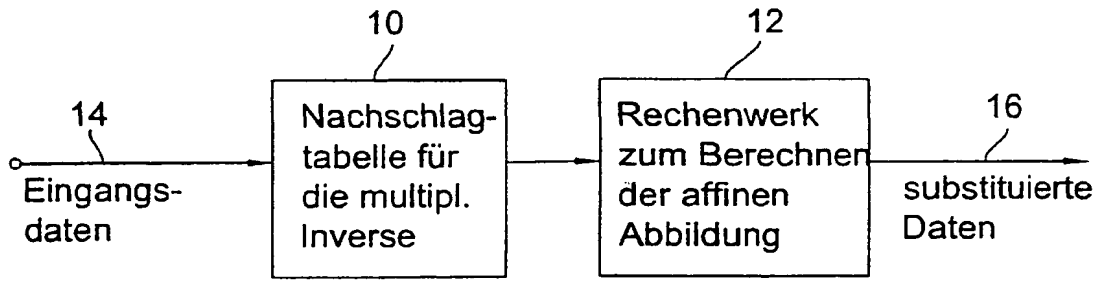
(74) Anwälte: **SCHOPPE, Fritz** usw.; Schoppe, Zimmermann, Stöckeler & Zinkler, Postfach 71 08 67, 81458 München (DE).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND DEVICE FOR EXECUTING A BYTE SUBSTITUTION OPERATION OF THE AES ALGORITHM ACCORDING TO RIJNDAEL

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUM AUSFÜHREN EINER BYTESUBSTITUTIONSOPERATION DES AES-ALGORITHMUS NACH RIJNDAEL



14 INPUT DATA

10 LOOK-UP TABLE FOR THE MULTIPLICATIVE INVERSE

12 ARITHMETIC-LOGIC UNIT FOR CALCULATING THE AFFINE MAPPING

16 SUBSTITUTED DATA

(57) Abstract: When executing a byte substitution operation of the AES algorithm according to Rijndael, whereby the byte substitution operation has a partial operation of the affine mapping and a partial operation of the multiplicative inverses, the partial operation of the multiplicative inverses is executed using a look-up table, whereas the partial operation of the affine mapping is calculated using a hardwired arithmetic-logic unit or in software. Instead of the S-box, only the multiplicative inverse is stored in tabular form so that the same look-up table can be used in a decrypting device and in an encrypting device of an AES cryptography system, whereby resulting in a savings in memory according to the size of the look-up table.

(57) Zusammenfassung: Beim Ausführen einer Bytesubstitutionsoperation des AES-Algorithmus nach Rijndael, wobei die Bytesubstitutionsoperation eine Teiloperation der affinen Abbildung und eine Teiloperation der multiplikativen Inversen aufweist, wird die Teiloperation der multiplikativen Inversen mittels einer Nachschlagtabelle ausgeführt, während die Teiloperation der affinen Abbildung mittels eines fest verdrahteten Rechenwerks oder in Software berechnet wird. Statt der S-Box wird nur noch die multiplikative Inverse tabellarisch

[Fortsetzung auf der nächsten Seite]

WO 03/010919 A1

CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:
— *mit internationalem Recherchenbericht*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

gespeichert, so daß in einer Entschlüsselungseinrichtung und einer Verschlüsselungseinrichtung eines AES-Kryptographiesystems dieselbe Nachschlagtabelle verwendet werden kann, was in einer Speichereinsparung entsprechend der Größe einer Nachschlagtabelle resultiert.

XCID <WO_03010919A1_I_>

Beschreibung

Verfahren und Vorrichtung zum Ausführen einer Bytesubstitutionsoperation des AES-Algorithmus nach Rijndael

Die vorliegende Erfindung bezieht sich auf den AES-Algorithmus nach Rijndael und insbesondere auf eine verbesserte Implementation der Bytesubstitutionsoperation dieses Algorithmus.

Fig. 6 zeigt ein Übersichtsdiagramm für den AES-Kryptoalgorithmus, der auch als Rijndael-Algorithmus bezeichnet wird. Der Rijndael-Algorithmus ist in dem Dokument „The Rjindael Block Cipher: AES Proposal" von Joan Daemen und Vincent Rijmen, Document Version 2, 9. März 1999, beschrieben. Der AES-Algorithmus ist ein iterativer Algorithmus, bei dem eine vorgegebene Anzahl (10, 12 oder 14) von Runden (rounds) berechnet wird. Nachfolgend wird anhand von Fig. 6 eine Runde des AES-Algorithmus für einen Modus exemplarisch dargestellt. Startpunkt einer Runde ist ein Block von 16 Bytes, wobei jedes Byte 8 Bit umfaßt, also ein Block von 8 x 16 Bits. Diese sind in Fig. 6 bei 600 als vertikale Linien dargestellt. Der AES-Algorithmus oder Rijndael-Algorithmus ist ein sogenannter Block-Cipher-Algorithmus, bei dem bei dem in Fig. 6 gezeigten Beispiel ein Block von 16 x 8 Bits an Eingangsdaten gemeinsam verschlüsselt werden.

Der erste Schritt einer Runde wird als „Add Round Key" (Hinzufügen des Schlüssels für eine Runde) bezeichnet. Diese Funktion wird durch die bei 620 dargestellten Kreise symbolisiert. Der AES-Rundenschlüssel, der üblicherweise von einem AES-Schlüssel abgeleitet wird und als Expanded Key bezeichnet wird, umfaßt ebenfalls 16 x 8 Bit. In der Stufe Add Round Key wird eine bitweise XOR-Verschlüsselung mit dem AES-Rundenschlüssel und den 16 x 8 Bit an Eingangsdaten durchgeführt, wie es bei 630 dargestellt ist.

Die nächste Verarbeitungsstufe einer Runde des AES-Algorithmus besteht in einer Byte-Substitution, die in Fig. 6 als Byte-Sub bezeichnet wird. Die Byte-Substitution besteht in einer mathematischen Funktion, die beim AES-Algorithmus eine multiplikative Inverse mit affiner Abbildung umfaßt. Diese mathematische Funktion wird durch eine Nachschlagtabelle implementiert, welche üblicherweise als S-Box bezeichnet wird und in Fig. 6 durch Würfel 640 symbolisch dargestellt ist. Die Ausgangsdaten der Stufe 620 werden als Adresse für die S-Box, d. h. die Byte-Substitutions-Nachschlagtabelle, verwendet, um als Ausgangsdaten für jedes Byte ein Substitutionsbyte auszugeben, das die multiplikative Inverse mit affiner Abbildung der Eingangsadresse ist. Die S-Box enthält keine geheimen Informationen, sondern kann im voraus berechnet werden oder von einer öffentlich zugänglichen Stelle abgerufen werden. Die geheimen Informationen stecken in den Eingangsdaten, d. h. Eingangsadressen für die S-Box.

Die Ausgangsdaten der Byte-Substitution 640 werden dann einer Zeilenverschiebungsoperation 650 unterzogen, die in Fig. 6 als „Shift Row" bezeichnet wird. Die Ausgangsdaten der Stufe 650 werden dann einer Spaltenvermischung unterzogen, die in Fig. 6 durch längliche Quader symbolisch dargestellt ist und in der Technik als „Mix Column" bezeichnet wird. Die Operationen 620, 640, 650 und 660 bilden eine von typischerweise zehn Runden des AES-Algorithmus, wobei eine Runde in der Technik auch als Round bezeichnet wird. Die Ausgangsdaten der Mix-Column-Operation, d. h. einer Runde oder Round, werden dann wieder einer Add-Round-Key-Operation 620' unterzogen, wobei wieder eine bitweise XOR-Verknüpfung der Daten mit einem Schlüssel 630' für die nächste Runde durchgeführt wird etc. Nach einer wählbaren Anzahl von Runden, welche üblicherweise 10 beträgt, liegen dann die AES-verschlüsselten Daten vor.

Nachteilig an der oben beschriebenen Ausführung der Bytesubstitution mittels einer Nachschlagtabelle ist, daß in einer

Verschlüsselungseinrichtung, in der Eingangsdaten in substituierte Daten transformiert werden, also in der Einrichtung 640 von Fig. 6, eine andere Tabelle verwendet werden muß, als in einer Entschlüsselungseinrichtung, in der die korrespondierende inverse Operation des symmetrischen AES-Algorithmus, also eine Rücksubstitution der Daten, durchgeführt wird. Eine Vorrichtung, die sowohl eine Verschlüsselung als auch eine Entschlüsselung gemäß dem AES-Algorithmus nach Rijndael durchführt, benötigt somit zwei Nachschlagtabellen, nämlich eine für die Verschlüsselungskomponente und eine für die Entschlüsselungskomponente. Es sei darauf hingewiesen, daß die Bytesubstitutions-Nachschlagtabelle 256 x 8 Bits, also 256 Byte groß ist. Eine bekannte Vorrichtung benötigt daher 2 x 256 Byte Speicherplatz zum Speichern der Bytesubstitutionstabelle.

Die obigen Speicherangaben gelten für eine serielle Berechnung der Bytesubstitution. Aus Schnelligkeitsgründen wird jedoch üblicherweise eine parallele Verarbeitung der z. B. 16 Bytes eingesetzt. Dann muß die Bytesubstitutionstabelle 16-fach vorhanden sein. Der benötigte Speicherplatz beträgt dann 16 x 2 x 256 Byte.

Für Anwendungen des AES-Algorithmus auf Allzweckcomputern stellt dies kein wesentliches Problem dar. Ganz anders verhält sich die Situation jedoch bei Chipkarten, bei denen aufgrund der Größe des Speicherchips sehr restriktive Speicheranforderungen vorhanden sind. Der Speicher auf Chipkarten liegt im Bereich von Kilobyte, so daß die Bytesubstitutionstabellen für die Entschlüsselungskomponente als auch für die Verschlüsselungskomponente der Schaltung einen wesentlichen Speicherplatz in Anspruch nehmen. Andererseits sind die auf einer Chipkarte auszuführenden Algorithmen mehr und mehr komplex, so daß auch die Anforderungen hinsichtlich des Arbeitsspeichers der Chipkarte ansteigen, damit die Chipkarte auch komplexere Algorithmen mit einem vernünftigen Durchsatz berechnen kann.

Die Aufgabe der vorliegenden Erfindung besteht darin, ein effizienteres Konzept zum Ausführen einer Bytesubstitutionsoperation des AES-Algorithmus nach Rijndael zu schaffen.

Diese Aufgabe wird durch ein Verfahren gemäß Patentanspruch 1, durch eine Vorrichtung gemäß Patentanspruch 7 oder durch ein Kryptographiesystem gemäß Patentanspruch 8 gelöst.

Der vorliegenden Erfindung liegt die Erkenntnis zugrunde, daß die Bytesubstitutionsoperation z. B. des AES-Algorithmus nach Rijndael aufgesplittet werden muß und teils durch ein fest verdrahtetes Rechenwerk und teils z. B. durch eine Nachschlagtabelle oder anderweitig durchzuführen ist. Die Bytesubstitutionsoperation besteht aus zwei Teiloperationen, nämlich der Operation der multiplikativen Inversen und der Teiloperation der affinen Abbildung. In Analogie dazu besteht die Bytesubstitutionsoperation in einer Entschlüsselungsvorrichtung in einer Teiloperation der inversen affinen Abbildung und in der Teiloperation der multiplikativen Inversen.

Erfindungsgemäß wird die affine Abbildung mittels eines fest verdrahteten Rechenwerks ausgeführt, während die multiplikative Inverse z. B. mittels einer Nachschlagtabelle ermittelt wird. Dies ermöglicht es, daß sowohl für die Verschlüsselungsoperation als auch für die Entschlüsselungsoperation dieselbe Nachschlagtabelle verwendet werden kann, nämlich einfach die Nachschlagtabelle der multiplikativen Inversen. Eine Kryptographievorrichtung mit einer Entschlüsselungskomponente und einer Verschlüsselungskomponente muß daher lediglich noch eine einzige Nachschlagtabelle für die Bytesubstitutionsoperation speichern, was in einer Speichereinsparung von beispielsweise 16 x 256 Byte für eine parallele Implementation resultiert. Für größere Nachschlagtabellen, d. h., wenn der AES-Algorithmus nicht byteweise, sondern auf größere Datenblöcke ausgeführt wird, ist die Speichereinsparung in Byte noch signifikanter.

Falls die Berechnung der multiplikativen Inversen auf andere Weise als durch eine Nachschlagtabelle durchgeführt wird, so ist die vorliegende Erfindung vorteilhaft darin, daß z. B. nur ein einziges Rechenwerk oder nur ein einziges Softwareprogramm sowohl für die Verschlüsselung als auch die Entschlüsselung benötigt werden.

Erfindungsgemäß werden in der Nachschlagtabelle somit nicht die üblicherweise verfügbaren S-Box-Werte abgelegt, sondern lediglich eine Tabelle der multiplikativen Inversen der Eingangs- (Adreß-) Werte. In einem weiteren Schritt wird dann die affine Abbildung fest verdrahtet realisiert. Eine bevorzugte Verdrahtung besteht darin, lediglich XOR-Gatter zu verwenden, wobei in einer weiteren Ausgestaltung der vorliegenden Erfindung lediglich XOR-Gatter mit zwei Eingängen eingesetzt werden, um die Anzahl der nötigen Transistoren zu begrenzen.

Dadurch kann die gleiche Tabelle zum Verschlüsseln und Entschlüsseln verwendet werden und es müssen nicht zwei getrennte Tabellen mit 256 x 8 Bits gespeichert werden.

Bevorzugte Ausführungsbeispiele der vorliegenden Erfindung werden nachfolgend bezugnehmend auf die beiliegenden Zeichnungen näher erläutert. Es zeigen:

Fig. 1 ein Blockschaltbild einer erfindungsgemäßen Vorrichtung zum Ausführen einer Bytesubstitutionsoperation des AES-Algorithmus nach Rijndael für die Verschlüsselungsoperation;

Fig. 2 ein Blockschaltbild einer Vorrichtung zum Ausführen einer Bytesubstitutionsoperation des AES-Algorithmus nach Rijndael für die Entschlüsselungsoperation;

Fig. 3a die Rechenvorschrift für die affine Abbildung;

Fig. 3b eine arithmetisch-logische Darstellung der Vorschrift von Fig. 3a;

Fig. 4 ein Rechenwerk zum Berechnen der affinen Abbildung gemäß einem ersten Ausführungsbeispiel der vorliegenden Erfindung;

Fig. 5 ein Rechenwerk zum Berechnen der affinen Abbildung gemäß einem weiteren Ausführungsbeispiel der vorliegenden Erfindung; und

Fig. 6 ein Übersichtsdiagramm über eine Runde des AES-Algorithmus.

Die Bytesubstitutionsoperation des AES-Algorithmus ist eine nichtlineare Bytesubstitution, die auf jedes der Zustandsbytes des AES-Algorithmus unabhängig wirkt. Die Substitutionstabelle (oder S-Box) besteht aus zwei Transformationen. Zunächst muß die multiplikative Inverse in $GF(2^8)$ ermittelt werden, und dann müssen die Ergebnisdaten einer affinen Transformation (über GF(2)) unterzogen werden.

Erfindungsgemäß umfaßt die Vorrichtung zum Ausführen der Bytesubstitutionsoperation zunächst eine Einrichtung 10 zum Ausführen der Teiloperation der multiplikativen Inversen mittels einer Nachschlagtabelle und dann ein fest verdrahtetes Rechenwerk 12 zum Berechnen der affinen Abbildung der Ausgangsdaten der Einrichtung 10, um aus Eingangsdaten an einem Eingang 14 substituierte Daten an einem Ausgang 16 zu erhalten.

Während Fig. 1 für eine Verschlüsselungsvorrichtung gilt, ist Fig. 2 für eine Entschlüsselungsvorrichtung dargestellt. Substituierte Daten werden zunächst einem Rechenwerk 20, das fest verdrahtet ist, zugeführt. Das Rechenwerk berechnet die

inverse affine Abbildung. Die Ausgangsdaten der Einrichtung 20 werden dann einer Einrichtung 22 zum Berechnen der multiplikativen Inversen zugeführt. Die Einrichtung 22 ist wieder, wie die Einrichtung 10 von Fig. 1, als Nachschlagtabelle für die multiplikative Inverse organisiert. An einem Ausgang 24 der in Fig. 2 gezeigten Vorrichtung liegen somit rücksubstituierte Daten vor, die aus substituierten Daten an einem Eingang 26 der in Fig. 2 gezeigten Vorrichtung berechnet worden sind.

Im nachfolgenden wird bezugnehmend auf Fig. 3a auf die Berechnungsvorschrift zum Berechnen der affinen Abbildung eingegangen. Fig. 3a stellt somit die Rechenvorschrift dar, die das Rechenwerk 12 aus Fig. 1 umsetzen muß. Die Eingangsdaten in das Rechenwerk sind mit x_0 bis x_7 bezeichnet, während die Ausgangsdaten aus dem Rechenwerk, also die substituierten Daten von Fig. 1, mit y_0 bis y_7 bezeichnet sind. Es sei darauf hingewiesen, daß die affine Abbildung in Fig. 3a für acht Eingangsbits und acht Ausgangsbits dargestellt ist. Es sei jedoch auch darauf hingewiesen, daß der AES-Algorithmus prinzipiell auch mit einer anderen Anzahl von Bits pro Block implementiert werden könnte.

Durch Inversion der Vektorgleichung, die in Fig. 3a gezeigt ist, wird die mathematische Vorschrift zum Berechnen der inversen affinen Abbildung, die durch das Rechenwerk 20 von Fig. 2 zu implementieren ist, erhalten.

Fig. 3b zeigt die Berechnungsvorschrift der Gleichung von Fig. 3a mittels logischer Operatoren, wobei das Zeichen + für eine XOR-Verknüpfung steht, während das Zeichen - für eine NICHT- oder NOT-Operation steht. Die Addition, die durch die letzte Spalte von Fig. 3a dargestellt ist, kann im Dualsystem auch durch die NOT-Operation berechnet werden, je nachdem, was schaltungstechnisch günstiger ist.

Fig. 4 zeigt eine schaltungstechnische Realisierung der in Fig. 3b gezeigten Gleichungen. Als Eingangswerte werden x_0 bis x_7 eingegeben, um als Ausgangswerte y_0 bis y_7 zu erhalten. Die in Fig. 4 gezeigte Schaltung umfaßt acht XOR-Gatter 40 bis 47, wobei die Ausgänge der XOR-Gatter 40, 41, 45 und 46, wie es durch die in Fig. 3b gezeigten entsprechenden Gleichungen vorgegeben ist, invertiert sind.

Wie es aus Fig. 4 zu sehen ist, hat jedes der XOR-Gatter 40 bis 47 mehr als zwei Eingänge.

Eine Transistor-sparendere Implementation der in Fig. 3b gezeigten Berechnungsvorschrift ist in Fig. 5 dargestellt. Fig. 5 umfaßt wieder ausschließlich XOR-Gatter 50 bis 65, wobei jedoch sämtliche Gatter ausschließlich zwei Eingänge und einen Ausgang haben. Mittels der XOR-Gatter 50 bis 53 werden erste Hilfsgrößen H1 bis H4 berechnet. Mittels der XOR-Gatter 54 bis 57 werden dann aus den ersten Hilfsgrößen H1 bis H4 zweite Hilfsgrößen H5 bis H8 berechnet. Die Ausgangswerte, also die substituierten Daten am Ausgang 16 von Fig. 1 bzw. y_0 bis y_7, werden schließlich durch die XOR-Gatter 58 bis 65 erhalten, wobei die Ausgänge der XOR-Gatter 58, 59, 63 und 64 invertiert sind, wie es durch die in Fig. 3b gezeigten Gleichungen vorgegeben ist.

Obgleich die in Fig. 5 gezeigte Schaltung mehr XOR-Gatter als die in Fig. 4 gezeigte Schaltung aufweist, wird sie dennoch bevorzugt, da jedes der in Fig. 5 gezeigten XOR-Gatter lediglich zwei Eingänge aufweist, so daß insgesamt eine Transistoreinsparung erreicht werden kann.

Es sei darauf hingewiesen, daß weitere schaltungstechnische Implementationen der Teiloperation der affinen Abbildung bzw. der inversen affinen Abbildung implementiert werden können. Unabhängig davon, welche spezielle Implementation für das fest verdrahtete Rechenwerk zum Berechnen der affinen Abbildung gewählt wird, oder ob die Berechnung der affinen Abbil-

dung softwaremäßig implementiert wird, wird immer der Vorteil erhalten, daß sowohl die Entschlüsselungskomponente als auch die Verschlüsselungskomponente einer Kryptographievorrichtung dieselbe Nachschlagtabelle verwenden können, in der die multiplikative Inverse tabellarisch abgespeichert ist.

Bezugszeichenliste

10 Einrichtung zum Ausführen der Teiloperation der multiplikativen Inversen
12 Rechenwerk zum Berechnen der affinen Abbildung
14 Eingang einer Verschlüsselungseinrichtung
16 Ausgang der Verschlüsselungseinrichtung
20 Rechenwerk zum Berechnen der inversen affinen Abbildung
22 Einrichtung zum Ausführen der Teiloperation der multiplikativen Inversen mittels einer Nachschlagtabelle
24 Ausgang der Entschlüsselungseinrichtung
26 Eingang der Entschlüsselungseinrichtung
40 - 47 XOR-Gatter mit mehr als zwei Eingängen
50 - 57 erster Satz von XOR-Gattern mit zwei Eingängen
58 - 65 zweiter Satz von XOR-Gattern mit zwei Eingängen
600 Eingangsbyte
620 Add-Round-Key-Funktion
630 XOR-Verschlüsselung mit dem AES-Rundenschlüssel
640 Bytesubstitutionsoperation mittels einer S-Box
650 Shift-Row-Funktion
660 Mix-Column-Funktion
620' Add-Round-Key-Funktion der nächsten Runde
630' XOR-Verschlüsselung für die nächste Runde

Patentansprüche

1. Verfahren zum Ausführen einer Bytesubstitutionsoperation, wobei die Bytesubstitutionsoperation eine Teiloperation der affinen Abbildung und eine Teiloperation der multiplikativen Inversen aufweist, mit folgenden Schritten:

Ausführen (10) der Teiloperation der multiplikativen Inversen; und

Ausführen (12) der Teiloperation der affinen Abbildung mittels eines Rechenwerks.

2. Verfahren nach Anspruch 1, bei dem die Bytesubstitutionsoperation die Bytesubstitutionsoperation des AES-Algorithmus nach Rijndael ist.

3. Verfahren nach Anspruch 1 oder 2, bei dem der Schritt des Ausführens (10) der Teiloperation der multiplikativen Inversen mittels einer Nachschlagtabelle durchgeführt wird.

4. Verfahren gemäß einem der vorhergehenden Ansprüche, bei dem das Rechenwerk zum Berechnen der Teiloperation der affinen Abbildung eine CPU ist und die Berechnung in Software ausgeführt wird.

5. Verfahren gemäß einem der Ansprüche 1 bis 3, bei dem das Rechenwerk zum Berechnen der affinen Abbildung ein fest verdrahtetes Rechenwerk ist.

6. Verfahren gemäß Anspruch 5, bei dem das fest verdrahtete Rechenwerk zum Ausführen der Teiloperation der affinen Abbildung lediglich XOR-Gatter aufweist.

7. Verfahren gemäß Anspruch 6, bei dem jedes XOR-Gatter des fest verdrahteten Rechenwerks lediglich zwei Eingänge und einen Ausgang aufweist.

8. Verfahren gemäß Anspruch 7,

bei dem ein Dateneingangsblock für die Bytesubstitutionsoperation eine Anzahl von Bits aufweist und ein Datenausgangsblock für die Bytesubstitutionsoperation dieselbe Anzahl von Bits aufweist, und

bei dem der Schritt des Ausführens der Teiloperation der affinen Abbildung folgende Schritte aufweist:

Berechnen einer Anzahl von Hilfsgrößen (H1 - H8) unter Verwendung eines ersten Satzes von XOR-Gattern (50 - 57) mit jeweils genau zwei Eingängen, dessen Anzahl gleich der Anzahl der Hilfsgrößen ist, wobei die Anzahl der Hilfsgrößen gleich der Anzahl von Bits des Dateneingangsblocks ist; und

Berechnen der Bits (y_0 - y_7) des Datenausgangsblocks unter Verwendung eines zweiten Satzes von XOR-Gattern (58 - 65) mit jeweils zwei Eingängen unter Verwendung der Bits des Dateneingangsblocks und der Hilfsgrößen, wobei die Anzahl der XOR-Gatter (58 - 65) des zweiten Satzes gleich der Anzahl von Bits des Datenausgangsblocks ist.

9. Vorrichtung zum Ausführen einer Bytesubstitutionsoperation, wobei die Bytesubstitutionsoperation eine Teiloperation der affinen Abbildung und eine Teiloperation der multiplikativen Inversen aufweist, mit folgenden Merkmalen:

einer Einrichtung zum Ausführen (10) der Teiloperation der multiplikativen Inversen; und

einer Einrichtung zum Ausführen (12) der Teiloperation der affinen Abbildung mittels eines Rechenwerks.

10. Symmetrisches Kryptographiesystem zum Ausführen einer Verschlüsselungsoperation und einer Entschlüsselungsoperation

unter Verwendung eines Algorithmus, der eine Bytesubstitutionsoperation aufweist, die eine Teiloperation der affinen Abbildung und eine Teiloperation der multiplikativen Inversen aufweist, mit folgenden Merkmalen:

in einer Verschlüsselungseinrichtung:

eine Einrichtung zum Ausführen der Teiloperation der multiplikativen Inversen; und

ein Rechenwerk (12) zum Ausführen der Teiloperation der affinen Abbildung;

in einer Entschlüsselungseinrichtung:

ein Rechenwerk (20) zum Ausführen einer Operation, die zur Teiloperation der affinen Abbildung invers ist; und

eine Einrichtung (22) zum Ausführen der Teiloperation der multiplikativen Inversen,

wobei die Einrichtung (10) zum Ausführen der Teiloperation der multiplikativen Inversen in der Verschlüsselungseinrichtung und der Entschlüsselungseinrichtung ausgebildet sind, um gemeinsam eine einzige Einrichtung zu verwenden, durch die die Teiloperation der multiplikativen Inversen bestimmbar ist.

11. Symmetrisches Kryptographiesystem nach Anspruch 10, bei dem die einzige Einrichtung eine einzige Nachschlagtabelle aufweist, in der die Teiloperation der multiplikativen Inversen tabellarisch gespeichert ist

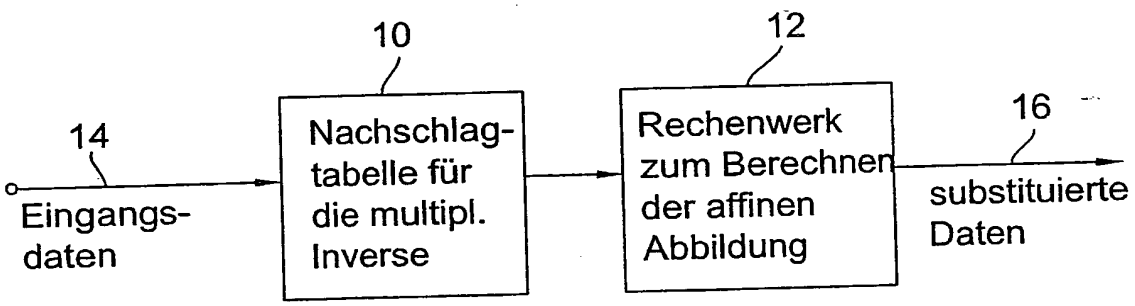

10
12
14
16
Nachschlag-
tabelle für
die multipl.
Inverse
Rechenwerk
zum Berechnen
der affinen
Abbildung
Eingangs-
daten
substituierte
Daten

FIG 1

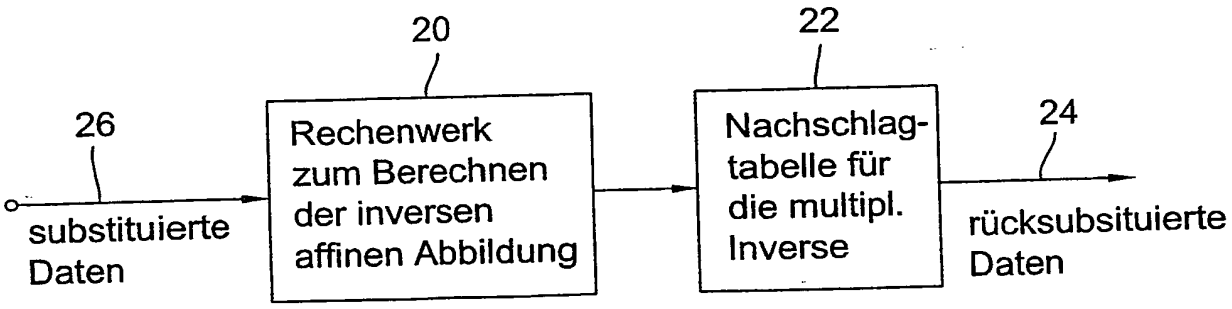

20
22
26
24
Rechenwerk
zum Berechnen
der inversen
affinen Abbildung
Nachschlag-
tabelle für
die multipl.
Inverse
substituierte
Daten
rücksubsituierte
Daten

FIG 2

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

FIG 3A

$$\begin{aligned} y_0 &= \ominus (x_0 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7) \\ y_1 &= \ominus (x_0 \oplus x_1 \oplus x_5 \oplus x_6 \oplus x_7) \\ y_2 &= \quad (x_0 \oplus x_1 \oplus x_2 \oplus x_6 \oplus x_7) \\ y_3 &= \quad (x_0 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_7) \\ y_4 &= \quad (x_0 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4) \\ y_5 &= \ominus (x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5) \\ y_6 &= \ominus (x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6) \\ y_7 &= \quad (x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7) \end{aligned}$$

FIG 3B

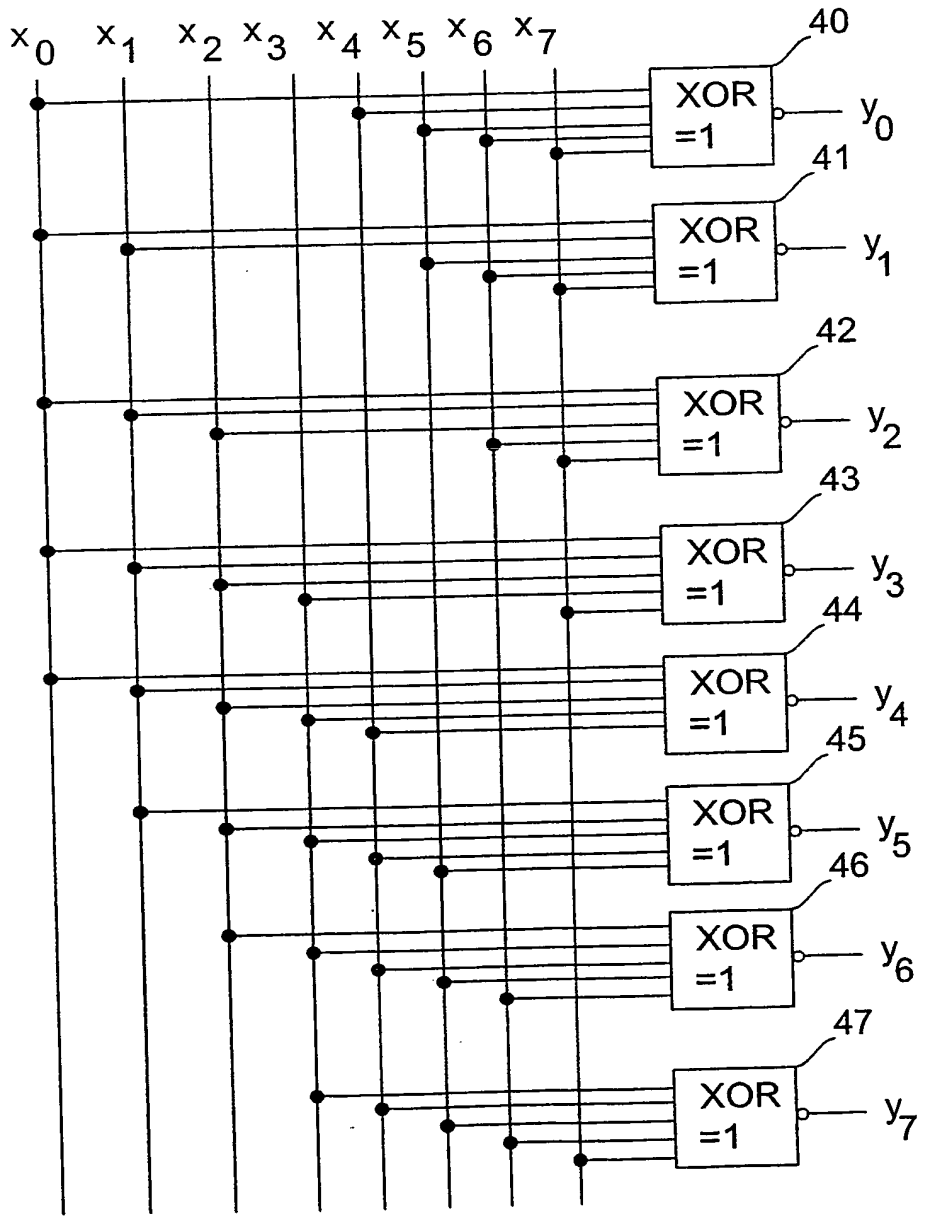

x0 x1 x2 x3 x4 x5 x6 x7
40
XOR =1
y0
41
XOR =1
y1
42
XOR =1
y2
43
XOR =1
y3
44
XOR =1
y4
45
XOR =1
y5
46
XOR =1
y6
47
XOR =1
y7

FIG 4

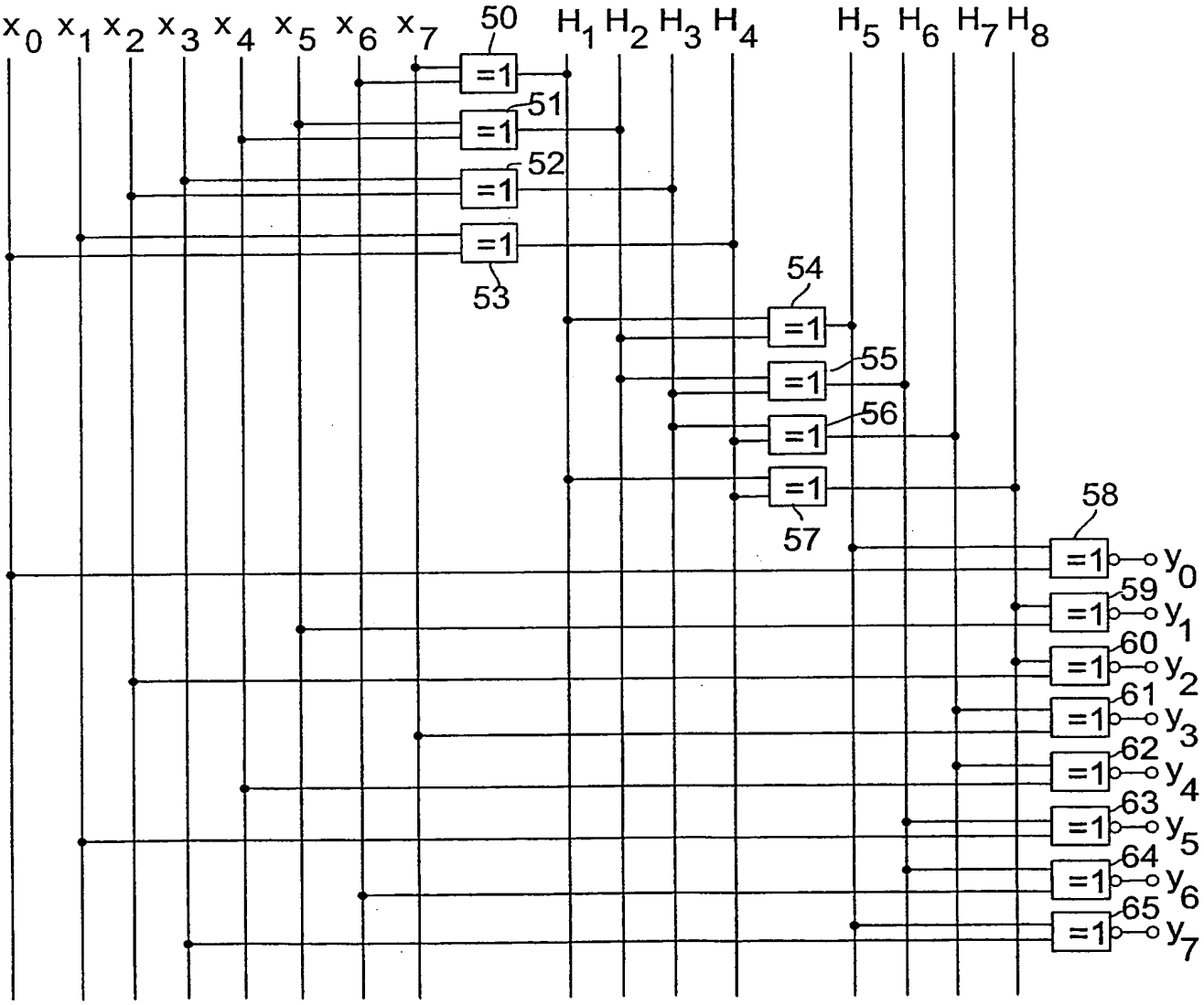


FIG 5

XOCID: <WO_03010919A1_I_>

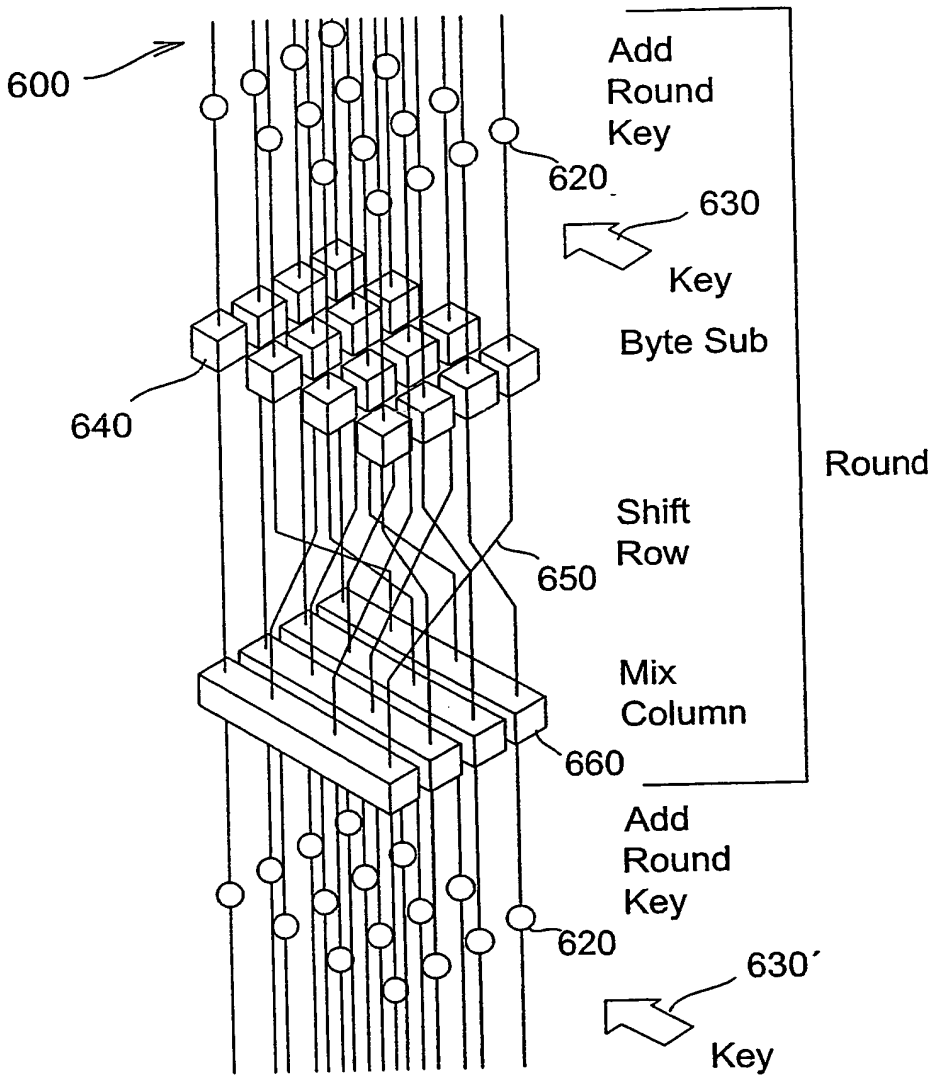


FIG 6
(STAND DER TECHNIK)

INTERNATIONAL SEARCH REPORT

	ıtional Application No
	PCT/EP 02/07296

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"Kryptografie" INTERNET, 'Online! XP002212728 Retrieved from the Internet: <URL:http://home.datacomm.ch/th.aes/Daten/Html/frame.html> 'retrieved on 2002-09-06! the whole document & "AES Algorithm Information" INTERNET, 'Online! 14 January 2000 (2000-01-14), Retrieved from the Internet: <URL:http://csrc.nist.gov/encryption/aes/rijndael/> 'retrieved on 2002-09-06! ---- -/--	1-11

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 September 2002	21/11/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Pfab, S

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	"AES" INTERNET, 'Online! XP002212729 Retrieved from the Internet: <URL:http://www.cs.fhm.edu/{koehler/krypto SS01/AES.pdf> 'retrieved on 2002-09-06! the whole document & "AES Algorithm Information" INTERNET, 'Online! 14 January 2000 (2000-01-14), Retrieved from the Internet: <URL:http://csrc.nist.gov/encryption/aes/r ijndael/> 'retrieved on 2002-09-06!	1-11
X	US 6 246 768 B1 (KIM YONG-DUK) 12 June 2001 (2001-06-12) abstract; figure 2 column 3, line 35 -column 5, line 33	1-11

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 02/07296

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6246768 B1	12-06-2001	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 02/07296

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/06

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	"Kryptografie" INTERNET, 'Online! XP002212728 Gefunden im Internet: <URL:http://home.datacomm.ch/th.aes/Daten/Html/frame.html> 'gefunden am 2002-09-06! das ganze Dokument & "AES Algorithm Information" INTERNET, 'Online! 14. Januar 2000 (2000-01-14), Gefunden im Internet: <URL:http://csrc.nist.gov/encryption/aes/rijndael/> 'gefunden am 2002-09-06! --- -/--	1-11

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
6. September 2002	21/11/2002

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax (+31–70) 340–3016	Pfab, S

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	"AES" INTERNET, 'Online! XP002212729 Gefunden im Internet: <URL:http://www.cs.fhm.edu/{koehler/krypto SS01/AES.pdf> 'gefunden am 2002-09-06! das ganze Dokument & "AES Algorithm Information" INTERNET, 'Online! 14. Januar 2000 (2000-01-14), Gefunden im Internet: <URL:http://csrc.nist.gov/encryption/aes/r ijndael/> 'gefunden am 2002-09-06!	1-11
X	US 6 246 768 B1 (KIM YONG-DUK) 12. Juni 2001 (2001-06-12) Zusammenfassung; Abbildung 2 Spalte 3, Zeile 35 -Spalte 5, Zeile 33	1-11

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentli jen, die zur selben Patentfamilie gehören

ıtionales Aktenzeichen
PCT/EP 02/07296

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 6246768 B1	12-06-2001	KEINE	